2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Law of the Horse to Law of the Submarine: The Future of State Behavior in Cyberspace

Paul A. Walker
Commander
U.S. Navy, Judge Advocate
General's Corps (Retired)
Washington, DC
Paul.walker@1987.usna.com

Abstract: States are rapidly approaching an international law crossroads in cyberspace. While many States, led by the United States, take the view that existing international law, including the law of armed conflict, is sufficient to cover cyberspace ("law of the horse"), such a view is being overtaken by reality. The Sony hack allegedly by North Korea is only the latest, and most blatant, in the long history of State activity in cyberspace. The current architecture of cyberspace makes it very attractive for States to pursue their national interests via this domain in a manner that is easily denied. With such a state of affairs persisting into the foreseeable future, it is very likely that international law will soon be sidelined or ignored by States as they seek to respond to cyber activity undertaken by other States ("law of the submarine"). With most, if not all, State-sponsored cyber activity not rising to the level of a use of force, countermeasures are one of the most viable international law tools for States to respond to State-sponsored cyber activity. Countermeasures, however, is the international law concept most at risk of being ignored by States. The customary international law of countermeasures imposes many conditions and limitations on their use, conditions and limitations that States will be inclined to ignore because they can under cyberspace's current architecture. Fortunately, the customary international law of countermeasures remains fluid enough that it can be sufficiently adapted to accommodate State behavior in cyberspace while still accounting for the international law interests underlying countermeasures.

Keywords: *international law, countermeasures, cyber activity, State action*

1. INTRODUCTION

"We will respond proportionally [to North Korea's hack of Sony], and we'll respond in a place and time and manner that we choose." – President Obama, December 19, 2014[1]

North Korea's alleged hack of Sony Pictures Entertainment is only the most recent – and most blatant – example of a State using cyberspace to pursue its national interests. Nation-States are suspected of actions against other nation-States as far back as the "Moonlight Maze" series of intrusions in 1999.[2] But beginning with Estonia in 2007,[3] alleged State actions have become increasingly visible. In addition, from Estonia (2007) to Georgia (2008)[4] to Stuxnet (2010-11)[5] to Saudi ARAMCO (2012)[6] to denials of service against U.S. banks (2012-13)[7] to Sony (2014)[8], one can trace a nearly linear line of increasingly disruptive, and potentially destructive, activity that is "attributed" to nation-States. Yet, no State has admitted undertaking these actions and no entity has provided absolute proof that a State was behind any of these malicious cyber actions. Taken alone, none of these events rises to the level of the cyber "pearl harbor" that is so often trumpeted.[9] Unfortunately, although international law is well-equipped to deal with a cyber "pearl harbor," it is not as well-equipped to deal with the current situation of unacknowledged and unattributed State actions not amounting to a use of force or an armed attack in cyberspace. This paper proposes modifications to the customary international law of countermeasures that are necessary to redress that deficiency in international law.

Modifications are necessary because the current architecture of cyberspace makes it very attractive for States to ignore international law. The internet's architecture makes it easy for States to achieve national security objectives through the interconnectedness of cyberspace, while maintaining the ability to deny their actions. The concept of deniability extends well beyond the usual problems of attribution and is particularly useful for States. Even when a State

1 Remarks by the President in Year-End Press Conference, The White House, Dec. 19, 2014, available at http://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.

2 Bob Drogin, *Russians Seem To Be Hacking Into Pentagon*, SFGATE, Oct. 7, 1999, at http://www.sfgate.com/news/article/Russians-Seem-To-Be-Hacking-Into-Pentagon-2903309.php.

3 *See, e.g.*, Eneken Tikk, Kadri Kaska and Liis Vihul, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 18-24 (2010) (describing the distributed denial of service actions against Estonia and their effects), available at https://ccdcoe.org/sites/default/files/multimedia/pdf/legalconsiderations_0.pdf.

4 *See, e.g.*, John Bumgarner & Scott Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, A US-CCU Special Report, 6 (Aug. 2009).

5 *See generally* Kim Zetter, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON (2014); *see also* David Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, Jun. 1, 2012 at A1 (citing anonymous sources attributing Stuxnet to the U.S. and Israel as part of a program named "Olympic Games").

6 *See, e.g.*, Byron Acohido, *Why the Shamoon Virus Looms as a Destructive Threat*, USA TODAY, May 16, 2013, available at http://www.usatoday.com/story/cybertruth/2013/05/16/shamoon-cyber-warfare-hackers-anti-american/2166147/.

7 Ellen Nakashima, *U.S. Rallied Multinational Response to 2012 Cyberattack on American Banks*, WASH. POST, Apr. 11, 2014, available at http://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html.

8 *See, e.g.*, Federal Bureau of Investigation, Update of Sony Investigation, FBI National Press Office, Dec. 19, 2014, at http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

9 *See, e.g.*, Leon E. Panetta, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, Oct. 11, 2013 ("The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life."), at http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

makes a prompt, public and affirmative attribution of cyberspace activity to another State[10], it is difficult to demonstrate and ensure the accuracy of that attribution[11] and the offending State still has the ability to deny responsibility. Because of the interconnected, global nature of the internet, States are able to achieve effects remotely, without placing personnel or other assets at physical risk.[12] As a result, States of all sizes are finding it easier than ever to accomplish national security objectives, whether disrupting an adversary's propaganda efforts,[13] sending active and visible messages of their own,[14] conducting aggressive intelligence collection[15] or conducting support to military operations[16] and sabotage.[17]

This paper begins with a brief overview of the positions that the leading States have taken with regard to the applicability of international law in cyberspace. Although Russia and the United States have long differed over the need for a treaty for cyberspace, the prevailing view, as articulated by the United States, is that existing international law norms are sufficient for addressing State activity in cyberspace. Such a position, though, is at odds with the apparent behaviour of States in cyberspace, where national interests are pursued without fear of responsibility or accountability. The next section examines a similar historical example where international law did not keep pace with technological developments and State practice, leading to the declaration of unrestricted submarine warfare by the U.S. immediately upon entry into World War II, an action not consistent with then-prevailing international law. Next, the difficulties of applying the customary international law of countermeasures in cyberspace are examined. The final section of the paper proposes modifications to the customary international law of countermeasures designed to accommodate State behaviour while still accounting for the international law interests underlying countermeasures.

2. "LAW OF THE HORSE" OR WHAT STATES SAY

In 1996, Judge Frank Easterbrook delivered a seminal lecture at the University of Chicago ostensibly about "Property in Cyberspace."[18] Judge Easterbrook took the opportunity to

10 The leading example is the U.S. attribution of the Sony hack to North Korea. *See* Federal Bureau of Investigation, Update of Sony Investigation, FBI National Press Office, Dec. 19, 2014, at http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

11 See *infra* note 60-61, and accompanying text.

12 *See, e.g.*, Elizabeth Flock, *Operation Cupcake: MI6 Replaces al-Qaeda Bomb-Making Instructions with Cupcake Recipes*, WASH. POST, Jun. 3, 2011 (describing efforts by the United Kingdom to disrupt the publication of al Qaeda in the Arabian Peninsula's *Inspire* magazine), at http://www.washingtonpost.com/blogs/worldviews/post/operation-cupcake-mi6-replaces-al-qaeda-bomb-making-instructions-with-cupcake-recipes/2011/06/03/AGFUP2HH_blog.html.

13 *See, e.g.*, Ellen Nakashima, *Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Cyberwar Policies*, WASH. POST, Mar. 19, 2010 at A1.

14 *See, e.g.*, Acohido, *supra* note 6 (describing the Shamoon virus as an Iranian response to a wiper virus used against Iran's oil industry); Ben Elgin and Michael Riley, *Now at the Sands Casino: An Iranian Hacker in Every Server*, BloombergBusiness, Dec. 11, 2014 (describing an alleged Iranian action against Sands Casino because of anti-Iranian statement made by the casino's owner), available at http://www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas.

15 *See, e.g.*, Michael Riley, *How Russian Hackers Stole the NASDAQ*, BUSINESS WEEK, Jul. 17, 2014 ("By mid-2011, investigators began to conclude that the Russians weren't trying to sabotage Nasdaq. They wanted to clone it, either to incorporate its technology directly into their exchange or as a model to learn from.").

16 *See* Bumgarner & Borg, *supra* note 4, at 6.

17 *See generally* Zetter, *supra* note 5; *see also* Sanger, *supra* note 5, at A1 (citing anonymous sources attributing Stuxnet to the U.S. and Israel as part of a program named "Olympic Games").

18 *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207.

question the very premise not only of his assigned topic, but the underlying premise of the conference that there was a need to adapt law for cyberspace.[19] Instead, Judge Easterbrook advocated for the application of existing legal principles to cyberspace.[20] He pointed to the fact that law schools do not teach a "law of the horse," as an analogy, arguing that "the best way to learn the law applicable to specialized endeavors is to study general rules" rather than trying to pull the strands of various areas of law (i.e., torts and contracts) into a "Law of the Horse" course.[21] Importantly, Judge Easterbrook did recognize that existing law is often flawed, even in the way that it applies outside of cyberspace.[22] Accordingly, he suggested that cyberspace could act as a type of catalyst to ensure the refinement of existing law through the implementation of sound principles that can be applied both outside and inside cyberspace.[23]

Despite the strength of his logic, Judge Easterbrook's position was strongly challenged by internet advocates, such as Lawrence Lessig.[24] Today, there are a number of legal texts dealing with "Cyberlaw" and many law schools have a similarly-titled course. Today, Judge Easterbrook's position finds much more support in the application of existing international law principles to cyberspace. The leading proponent of this view is the United States.

In 2011, the U.S. issued its *International Strategy for Cybersecurity*,[25] one of the first countries to do so. With respect to international law, the U.S. strategy stated there was no need to reinvent international law and that international norms are not "obsolete."[26] Although acknowledging the need for "additional work" to clarify how these norms apply in cyberspace, "[l]ong-standing international norms guiding State behavior – in times of peace and conflict – also apply in cyberspace."[27] The U.S. position was further clarified publicly by Harold Koh, then the U.S. State Department's Legal Adviser. In a speech to the U.S. Cyber Command legal conference in September, 2012, Koh affirmed that international law does apply in cyberspace.[28] But he also went a step further. Alluding to Russian proposals for a new treaty to apply to the "cutting edge issues presented by the internet," Koh decisively rejected the need for new international law based on the uniqueness of cyberspace: "Some have also said that existing international law is not up to the task, and that we need entirely new treaties to impose a unique set of rules on cyberspace. But the United States has made clear our view that established principles of international law do apply in cyberspace."[29] In short, the "law of the horse" is rejected; what we have is good enough as long as we apply it properly.

Unfortunately, agreement on how international norms apply in cyberspace has been slow to develop. It was only in 2013 that the United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, a group that included Russia and China in addition to the U.S., were able

19 *Id.*
20 *Id*. at 208.
21 *Id*. at 207.
22 *Id*. at 209.
23 *Id*.
24 *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, HARV. L. REV. 501 (1999).
25 White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, May 2011.
26 *Id*. at 9.
27 *Id*.
28 Harold Hongju Koh, International Law in Cyberspace: Remarks to the USCYBERCOM Inter-Agency Legal Conference, Sept. 18, 2012, available at http://www.State.gov/s/l/releases/remarks/197924.htm.
29 *Id*.

to report agreement that international law and the UN Charter were applicable to cyberspace.[30] The 2010 report from the same group was unable to reach agreement on that point. Even with the publication of the 2013 report, there is still disagreement over the application of international law in cyberspace. Russia is still interested in implementing this concept via a new treaty. China, meanwhile, remains distrustful of western efforts to apply international law to cyberspace, denigrating efforts such as the Tallinn Manual for providing too permissive an atmosphere in cyberspace for the actions of western countries such as the United States.[31]

Despite agreement that international law applies in cyberspace, as discussed in the introduction there is growing evidence that States are behaving as if there are few, if any, restraints in the conduct of cyberspace activities.[32]

3. "LAW OF THE SUBMARINE" OR THE FUTURE OF STATE BEHAVIOR IN CYBERSPACE

States have ample incentive to pursue their national security interests via cyberspace in a manner that is not transparent. Some commentators correctly point out that the lack of transparency inhibits the development of international norms and the advancement of international law. Eichensehr, for instance, criticizes the fact that the U.S.'s 2011 *International Strategy for Cyberspace* does not adequately state what precise norms the United States is seeking.[33] As a result, the U.S. "is missing the opportunities to foster development of norms."[34] Jack Goldsmith also warns of the dangers of not being forthcoming with information: "[the FBI's] hesitation in the face of credible questions about its very thin public evidence will exacerbate the demand for publicly verifiable attribution before countermeasures (or other responses) are deemed legitimate."[35] But the failure to develop international norms of behaviour and advance the development of international is not the greatest danger to the international system of States' demonstrated behaviour in cyberspace. The greater danger is that international law will be ignored altogether, a situation that is not without precedent.

Within hours of the attack on Pearl Harbor, the U.S. Navy Chief of Naval Operations (CNO) knowingly ordered the Navy to violate international law by directing the use of unrestricted

30 United Nations, REPORT OF THE GROUP OF GOVERNMENTAL EXPERTS ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY, Jul. 30, 2013, at 2, available at http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

31 Adam Segal, NATO's *Take on Cyberspace Law Ruffles China's Feathers*, DEFENSE ONE, Oct. 29, 2014 (summarizing an article in the People's Liberation Army Daily critical of the Tallinn Manual "as an effort to manipulate cyberspace using law" and as a way for the U.S. to maintain its dominance).

32 See *supra* notes 10-17, and accompanying text.

33 Kristen Eichensehr, *The US Needs a New International Strategy for Cyberspace*, JUST SECURITY, Nov. 24, 2014, at http://justsecurity.org/17729/time-u-s-international-strategy-cyberspace/.

34 *Id*.

35 Jack Goldsmith, *The Consequences of Credible Doubt About the USG Attribution in the Sony Hack*, LAWFARE, Dec. 30, 2014, at http://www.lawfareblog.com/2014/12/the-consequences-of-credible-doubt-about-the-usg-attribution-in-the-sony-hack/.

submarine warfare against Japan.[36] International law then (and now) required submarines to remove a merchant vessel's crew to a place of safety before sinking the merchant vessel and a lifeboat on the open sea did not suffice as a place of safety.[37] These "cruiser rules," applying as they did to any merchant vessel regardless of whether it was flagged to a belligerent or a neutral,[38] were untenable for submarines, whose great advantage lay in the stealth and surprise afforded by hiding under the sea and who are very vulnerable on the surface.[39] Nor did submarines have sufficient manning to provide prize crews that could sail the merchant vessel to a friendly port. Faced with the irreconcilable difference between the dictates of international law and effective military strategy, Navy leaders chose to ignore international law.

Confronted with increasingly disruptive and frequent State activities in cyberspace, States today are confronting a similar dilemma. With all cyberspace activity to-date falling below the level of an armed attack[40] that would provide the ability to use force in self-defense, countermeasures are one of the most viable options for States to use in responding to current levels of State cyber activity. Yet, the current legal framework for countermeasures is not compatible with State's demonstrated behaviour in cyberspace.

4. THE COUNTERMEASURE DIFFICULTY

Countermeasures are State actions that would normally be considered a violation of international law, but become justified by the fact that they are undertaken in response to another State's internationally wrongful act.[41] It is generally understood that a proper countermeasure should not amount to a use of force and must not violate any other peremptory norm of international law.[42] Beyond network defense actions and multilateral efforts, there are a variety of active cyberspace-based responses that could be used as a countermeasure. One such countermeasure

36 Joel Ira Holwitt, "EXECUTE AGAINST JAPAN:" THE U.S. DECISION TO CONDUCT UNRESTRICTED SUBMARINE WARFARE 14 (2008). Although the CNO's order was issued roughly four-and-a-half hours after the attack on Pearl Harbor, his was not the first U.S. Navy order to do so. The Commander of the Asiatic Fleet, Admiral Hart, ordered his air and submarine units to carry out unrestricted warfare three hours earlier, but Admiral Hart knew that the CNO was going to issue the same order on the outbreak of hostilities. *Id*. at 156. The CNO's decision came after "a year of debate and consideration by the U.S. naval leadership." *Id*. at 15.

37 *Id*. at 58-59 (describing how only five years earlier the United States had signed the London Submarine Protocol, which re-affirmed Article 22 of the London Naval Treaty of 1930 requiring submarines to adhere to "cruiser rules" with respect to merchants).

38 *Id*.

39 *Id*. Holwitt points to an early article by a young Lieutenant Hyman Rickover, later the "father of the nuclear Navy," that succinctly makes the point: "The conclusion is inevitable that, except in rare circumstances, it is impossible for the submarine to carry on commerce warfare in accordance with international law as it stands today. Consequently, states must either renounce this weapon as a commerce destroyer or undertake a revision of the laws governing naval warfare, taking into account the changed conditions of modern war. . ." *Id*. at 61, quoting from H. G. Rickover, *International Law and the Submarine*, 61 PROCEEDINGS 1219 (Sept. 1935).

40 Michael N. Schmitt, ed., TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 57 (2013) [hereinafter TALLINN MANUAL] ("No international cyber incidents have, as of 2012, been unambiguously and publicly characterized by the international community as reaching the threshold of an armed attack."). There have been not been any that met this criteria in the years since, either.

41 Draft Articles on Responsibility of States for Internationally Wrongful Acts, International Law Commission, Art. 22 (2001) [hereinafter *Draft Articles*] ("The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State…").

42 *Id*. at 131, Art. 50.

is designed to get the offending activity to stop, or "cease and desist."[43] For example, an action that causes an offending web browser to close without affecting any other part of the computer.[44] Likewise, suborning a botnet's command and control channel and telling the botnet to shut itself off or to delete itself,[45] or to direct its activity at a sinkhole IP address[46] would be other examples of non-cooperative "cease and desist." A more active approach is what has come to be known as "hack back," which involves accessing the offending computer(s) for the purpose of retrieving stolen data by deleting it from the possession of the offender, deleting malicious programs, or corrupting, in a reversible manner, the computer(s) that is the origin of the offending cyber activity.[47] An active response not involving a "hack back" might involve the use of a distributed denial of service (DDoS) against an IP address or server that is the origin of malicious activity, or is controlling malicious activity, in order to prevent the activity from affecting the defender's system. By any reasonable measure, these kinds of actions are not forcible countermeasures. They do not result in deaths, injuries, or significant physical destruction,[48] nor do they reach the levels of severity, invasiveness, and measurability of effects, among other factors, that may lead to a use of force conclusion.[49]

The purpose of using a countermeasure is to effect a return to the *status quo ante*, that is, to get the offending State to resume its obligations under international law.[50] As such, the countermeasure(s) that a State undertakes should generally be temporary and reversible, so as not to create a permanent violation of international law.[51] This is a requirement that is easily met with cyberspace operations and is a key reason why cyberspace activity should be, and is, very attractive as a countermeasure. For instance, Heather Harrison Denniss notes that in 1998 the U.S. Department of Defense responded to "Floodnet" attacks against the Defense Department website with a program that closed the internet browser on the computers sending the "Floodnet" applet.[52] By generating this minimal result on all such computers, wherever located, the malicious activity against the website stopped. Although the action was taken against a non-state actor, Denniss views this outcome as an appropriate proportionate countermeasure.[53] While the temporary and reversible requirement for cyber countermeasures may not pose a difficulty, the same cannot be said of other limitations on countermeasures.

43 William A. Owen, Kenneth W. Dam, Herb Lin, eds., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 149 (2009) ("Non-cooperative 'cease and desist'" is "the use of tools to disable harmful services on the attacker's system without affecting other system services.").

44 Heather Harrison Denniss, CYBER WARFARE AND THE LAWS OF WAR 108 (2012), citing Brian Friel, DoD Launches Internet Counterattack, GOV'T EXECUTIVE (Sept. 18, 1998) (describing DoD action against malicious cyber activity in the late-1990s).

45 Paul Bacher, Thorsten Holz, Markus Kotter, Georg Wicherski, Know Your Enemy: Tracking Botnets (describing efforts to infiltrate BOTNETs using command and control channels), at https://www.honeynet.org/book/export/html/50.

46 Federal Bureau of Investigation, GameOver Zeus Botnet Disrupted (Jun. 2, 2014) (describing the use of " measures to sever communications between the infected computers, re-directing these computers away from criminal servers to substitute servers under the government's control").

47 Owen, Dam, & Lin, *supra* note 43, at 149.

48 Koh, *supra* note 28, at 3 (describing the U.S. position that cyber activity causing deaths, injuries or significant physical destruction is an illegal use of force).

49 TALLINN MANUAL, *supra* note 40, at 48-51 (discussing an approach designed "to assess the likelihood that States will characterize a cyber operation as a use of force), citing Michael N. Schmitt, *Computer Networks and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 914 (1999).

50 *Draft Articles, supra* note 41, at 129, Art. 49(1).

51 *Id*., Art. 49(3).

52 Denniss, *supra* note 44, at 108.

53 *Id*.

The customary international law of countermeasures imposes a number of limitations and conditions on the use of countermeasures. As an initial matter, countermeasures may only be taken "against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations" under international law.[54] In order to take countermeasures, therefore, a State is required to identify the State responsible for the internationally wrongful act. Once thought difficult, attribution of State action in cyberspace is becoming quite common. Anti-virus companies are at the forefront of these efforts, with the latest salvo a Kaspersky report identifying a group it calls the "Equation Group," which Kaspersky equates to the U.S.'s National Security Agency.[55] But States are beginning to publicly attribute internationally wrongful acts in cyberspace to other States, as well. Most prominently, in December, 2014, the United States made a prompt, public, affirmative statement[56] that North Korea was responsible for the hack of Sony Pictures Entertainment and the subsequent release of large quantities of company proprietary data and employee emails. Although North Korea has repeatedly and continuously denied this claim by the United States, the Federal Bureau of Investigation (FBI) claim is based on methodologies similar to those used by multiple anti-virus vendors in forensic reports claiming State sponsorship of cyber activity.

For instance, the FBI claimed that the command and control infrastructure used in the Sony hack overlapped "significant[ly]" with that observed in previous North Korean actions, including the use of internet protocol (IP) addresses "associated with known North Korean infrastructure" communicating with other IP addresses that were "hardcoded into the data deletion malware" used against Sony.[57] Mandiant and Kaspersky both made similar infrastructure claims in their reports attributing "APT 1" ("APT" stands for "advanced persistent threat") and Equation Group as the Chinese People's Liberation Army Unit 61398 and the U.S.'s National Security Agency, respectively.[58] Likewise, Mandiant, Kaspersky and FireEye (Mandiant's successor) also rely heavily on repeated uses of the same or similar software, often from software "families," which is not that different from the FBI's assertion that the data deletion malware was similar to "other malware that the FBI knows North Korean actors previously developed."[59] Despite these similarities to commonly used forensic methodologies, the U.S. attribution to

54 *Draft Articles, supra* note 41, Art. 49(1).

55 Dan Goodin, How "Omnipotent" Hackers Tied to NSA Hid for 14 Years—and Were Found at Last, Ars Technica (Feb 16, 2015), at http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/.

56 Federal Bureau of Investigation, Update of Sony Investigation, FBI National Press Office, Dec. 19, 2014, at http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

57 *Id*.

58 APT1: Exposing One of China's Cyberespionage Units, Mandiant 39-40 (describing infrastructure, including a large number of IP addresses and domain names, used by APT1 as hop points in their operations, with the activity leading back to four networks in the Shanghai area where Unit 61398 is based).

59 *Id*.

North Korea was not universally accepted by the information security community.[60] This may be due to the rapidity of the attribution claim, as well as the fact that it did not come in the type of lengthy and detailed report the industry is used to digesting. The failure to provide additional details undoubtedly accounts for a substantial portion of the negative reaction,[61] bolstered by the FBI's intimation that it relied on intelligence community sources not available to the information security community. Ultimately, though, it is up to the State to determine whether an internationally wrongful act has occurred and which State is responsible for that act, understanding that it may be held responsible for countermeasures taken erroneously.[62]

Once a State determines the State behind an internationally wrongful act, countermeasures may only be taken against that State. As the commentary to this portion of the Draft Articles on State Responsibility (Draft Articles) puts it, "Countermeasures may not be directed against States other than the responsible State."[63] Such a stricture presents particular difficulties in cyberspace when the offending activity may be initiated by a single State, but use infrastructure and equipment located in third States to carry out the cyber activity. As an example, the Iranian DDoS against U.S. bank websites used a network of compromised, linked computers (called a "botnet") to execute the DDoS action.[64] Most, if not all, of these computers were located in countries around the globe, not Iran. The owners of the compromised equipment, much less the State where geographically situated, had no idea they were compromised or the purpose for which they were used. Yet, to take action against these nodes of the botnet, even if it is the easiest, most temporary and reversible method, would seem to be precluded by the customary international law of countermeasures. The U.S. seems to agree with this approach, as when confronted with this situation, rather than acting unilaterally, it reached out to 120 nations in an effort to get those countries to directly address the offending behaviour.[65] Unfortunately, this effort did not lead to a significant diminution of the strength of the DDoS activity, which only ceased with a change in the Iranian domestic political situation.[66]

60 In addition to criticism of the FBI for relying on its own previous (unpublished) attribution, researchers also pointed out that the wiper malware used by North Korea was related to other such malware, including the Shamoon malware used against the Saudi ARAMCO oil company and widely attributed to Iran. Marc Rogers, Why I *still* Don't Think It's Likely that North Korea Hacked Sony, Marc's Security Ramblings, Dec. 21, 2014 (comparing Destover, the wiper malware used against Sony, to the Shamoon wiper malware used in Saudi Arabia and the Dark Seoul wiper malware used against South Korea), at http://marcrogers.org/2014/12/21/why-i-still-dont-think-its-likely-that-north-korea-hacked-sony/. *See also* Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know So Far*, WIRED, Dec. 3, 2014 (describing the use of the same commercially-available driver to do the wiping of data in Sony, Shamoon and Dark Seoul, which indicates not necessarily the same group, but easily copied techniques), at http://www.wired.com/2014/12/sony-hack-what-we-know/. Other criticism focused on how easily the IP addresses that were "associated" with North Korea could be spoofed or hacked. Kim Zetter, *Critics Say New Evidence Linking North Korea to the Sony Hack Is Still Flimsy*, WIRED, Jan. 8, 2015, at http://www.wired.com/2015/01/critics-say-new-north-korea-evidence-sony-still-flimsy/.

61 For instance, the FBI had a three-hour meeting with one cybersecurity firm that presented evidence the Sony hack was the work of "disgruntled" former Sony employees. *See* Tal Kopan, *U.S.: No Alternate Leads in Sony Hack*, POLITICO, Dec. 29, 2014 (describing the meeting between cyber intelligence company Norse and FBI officials), at http://www.politico.com/story/2014/12/fbi-briefed-on-alternate-sony-hack-theory-113866.html.

62 *Draft Articles*, supra note 41, at 130 ("A State which resorts to countermeasures based on its unilateral assessment of the situation does so at its own risk and may incur responsibility for its own wrongful conduct in the event of an incorrect assessment.").

63 *Id*. at 130.

64 Nakashima, *supra* note 7.

65 *Id*.

66 *Id*.

In addition to being taken against the offending State, countermeasures may only be undertaken while the internationally wrongful act is ongoing.[67] Once the internationally wrongful act has ceased, the countermeasure may not be initiated or, if already begun, must terminate.[68] This poses some difficulty in responding to cyberspace operations because often the internationally wrongful act may be a series of discreet acts or a single discreet event that, even when completed, may have ongoing repercussions. For instance, although the Iranian DDoS activity did not occur on a continual basis, it did periodically repeat itself for an extended period of time. The question then arises as to whether countermeasures may only be taken during an active DDoS event or could also occur in a lull so as to prevent another incident. Also problematic is the example of the Sony hack, where arguably North Korea's alleged internationally wrongful act ended up as a singular, completed event once the hackers announced their presence and absconded with Sony's proprietary information.

Given State behaviour in cyberspace as described in the introduction, particularly the demonstrated desire for deniability, the requirement to call upon the responsible State to fulfil its international law obligations is also problematic.[69] The purpose of this requirement is to give the offending State "notice of a claim and some opportunity to present a response" due to the "serious consequences of countermeasures."[70] The Commentary to the Draft Articles contemplates a period of "extensive and detailed" negotiations before the point of countermeasures is reached, with the notice requirement often inherent in these negotiations.[71] However, cyberspace activity will not generally lead to negotiations, given the deniability outcome. In fact, even when called upon to cease cyberspace activity, States such as China continue to deny their responsibility, even in the face of numerous well-sourced reports and indictments. Once States decide to undertake non-forcible countermeasures, there will usually be a need for much quicker action in the cyberspace domain. States may be unwilling to attribute internationally wrongful acts either publicly or directly to the State for fear of losing the ability to take effective countermeasures.

The second notice requirement, to inform the "responsible State of any decision to take countermeasures and offer to negotiate with that State"[72] is actually much less problematic because there is an "out" clause.[73] Specifically, this second notice provision is not required when the aggrieved State needs to take "urgent" countermeasures to preserve its rights, including its right to take countermeasures.[74] The out clause is provided in the event that notice to the offending State would allow it to take steps to "immunize" itself from the countermeasures.[75] In the case of cyber countermeasures, use of this exception will be a given in virtually every case in order to ensure chosen countermeasures remain effective.

67 *Draft Articles, supra* note 41, Art. 52(3)(a).
68 *Id*. at 136.
69 *Id*., Art. 52(1)(a).
70 *Id*. at 136.
71 *Id*.
72 *Id*., Art. 52(1)(b).
73 *Id*., Art. 52(3).
74 *Id*. at 136.
75 *Id*.

5. COUNTERMEASURES FOR THE DIGITAL AGE

There are three adjustments necessary to keep the customary international law of countermeasures relevant in the digital age. First, and most easily accomplished, the exception to the requirement to notify an offending State of the decision to take countermeasures should also apply to the requirement to call on the offending State to stop the international wrongful act. Instead, this requirement should be shifted to prompt notification *after* taking countermeasures. This change is necessitated by the need for States to retain the ability to take effective countermeasures. As seen with the Sony hack, even when one State implicates another in cyber activity that probably constitutes an internationally wrongful act, the nature of cyberspace is such that the accused State can plausibly continue to deny responsibility. Permitting States to wait until after-the-fact of countermeasures to call on a state to comply with its international obligations will encourage States to treat any response action they take not as punitive, but as a proper countermeasure, one which retains its effectiveness. Once the offending State is asked to resume its obligations under international law and learns of the fact of countermeasures, it then still has a full panoply of actions available to it under international law, including seeking redress for the countermeasure in an appropriate international forum. Of course, the preferred course of action by the offending State is to cease the original internationally wrongful act.

The second needed adjustment is clarification of when an internationally wrongful act in cyberspace ceases or is no longer ongoing. The focus of this limitation should not be on any single, discrete activity, but should focus on the broader failure of a State to live up to its obligations under international law on a continuing basis. As a result, countermeasures may then be available to a State during periods of inactivity, when there is a pattern of active and passive behaviour, or even after a discrete event when the effect of the discrete event is to support an ongoing wrong that is different in scope. For instance, in the case of the alleged Iranian DDoS activity against U.S. banks, once an active-inactive pattern is established, countermeasures could be taken during periods of inactivity in order to prevent further activity. In the case of the Sony hack, a case could be made that there is an ongoing violation of the non-intervention principle in the way that the alleged North Korean hackers are making use of the information to continue to harm Sony or other U.S. economic interests. In that instance, it may be appropriate to take a countermeasure designed to recover the stolen data by making it no longer useable by the hacker or to prevent its continued use in harming U.S. economic interests.

Finally, for countermeasures to remain a viable legal concept in cyberspace, they will need to remain effective as a practical matter, as well. To be effective, countermeasures in cyberspace will have to occur in the territory of third-party States. Note well, though, that while effective cyber countermeasures may need to occur *in* the territory of a third-party State, those countermeasures are not directed *against* that third-party State. Such countermeasures would remain directed against the cyber activities of the original, offending State, which itself is potentially committing an internationally wrongful act against the third-party State in the course of carrying out the activity against the receiving State. It is worth remembering, in that vein, that the cyber activity used to compromise equipment in that third-party State is usually occurring unbeknownst to the State or the owner of the equipment and thus neither

has any rational interest in the continued operation of the malware or exploit used to carry out the internationally wrongful act. Taking limited action to stop a botnet operation by using its own commands against it, including the possibility of telling it to delete itself, would not unduly impinge on core interests of the third-party State. Such action could easily be viewed as the type of "incidental" effects that typically occur in third States when one State takes economic countermeasures against another State. The Draft Articles use the suspension of a trade agreement as an example where one or more companies in third States "lose business or even go bankrupt" as a result of suspended trade with the responsible State. It is fair to say that a bankrupt company has a much greater impact on the third State's economy than simply deleting unknown and unwanted software or other minimal measures causing only temporary changes to the equipment, such as soft reboots.

6. CONCLUSION

State behaviour in cyberspace is going to look much like it has in the present and the past, including when using cyber measures to conduct countermeasures (or retaliation). States that are leaders in the area of cyberspace, such as the United States, are missing the opportunity to develop international norms. Moreover, there is great risk that the customary international law of countermeasures will be ignored altogether because it is too cumbersome to apply to cyberspace operations. Allowing States to take non-forcible cyber countermeasures against the effects of—or a pattern of—internationally wrongful acts, even if the countermeasure needs to occur in the cyber infrastructure of a third State followed by after-the-fact notification to those States, will keep the customary international law of countermeasures relevant for the digital age. These adjustments will also encourage more transparency by States, transparency that is urgently needed to advance legal discussion not only in the area of countermeasures, but all areas of international law impacted by State behaviour in cyberspace.